A Report
to the
Montana
Legislature

Performance Audit

Bankcard Transaction Fees and Contract Management

Department of Administration

June 2015

Legislative Audit
Division

14P-04

Performance Audits

Performance audits conducted by the Legislative Audit Division are designed to assess state government operations. From the audit work, a determination is made as to whether agencies and programs are accomplishing their purposes, and whether they can do so with greater efficiency and economy.

We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives. Members of the performance audit staff hold degrees in disciplines appropriate to the audit process.

Performance audits are performed at the request of the Legislative Audit Committee which is a bicameral and bipartisan standing committee of the Montana Legislature. The committee consists of six members of the Senate and six members of the House of Representatives.

Audit Staff

Katherine Guenther Joe Murray

Reports can be found in electronic format at:
http://leg.mt.gov/audit

LEGISLATIVE AUDIT DIVISION

Tori Hunthausen, Legislative Auditor
Deborah F. Butler, Legal Counsel

Deputy Legislative Auditors:
Cindy Jorgenson
Angus Maciver

June 2015

The Legislative Audit Committee
of the Montana State Legislature:

This is our performance audit on the accuracy and security of bankcard transactions processed at state agencies. The two term contracts used to process these transactions are managed by the Department of Administration.

This report provides the Legislature with information regarding the accuracy of point-of-sale and online transaction revenues and fees resulting from purchases made by customers for goods and services from state agencies. This report also provides information on the monitoring of contractors' security controls over the processing of sensitive and confidential bankcard information. This report includes recommendations for improving contract monitoring to better ensure the accuracy and security of bankcard transactions for the term contracts managed by the Department of Administration. A written response from the Department of Administration is included at the end of the report.

We wish to express our appreciation to Department of Administration personnel for their cooperation and assistance during the audit.

Respectfully submitted,

/s/ Tori Hunthausen

Tori Hunthausen, CPA
Legislative Auditor

Room 160 • State Capitol Building • PO Box 201705 • Helena, MT • 59620-1705
Phone (406) 444-3122 • FAX (406) 444-9784 • E-Mail lad@mt.gov

Table of Contents

Figures and Tables

Figures

Tables

Appointed and Administrative Officials

Department of Administration

Sheila Hogan, Director

Mike Manion, Deputy Director

Ron Baldwin, Chief Information Officer

Tammy LaVigne, Chief Intergovernmental Relations Officer

Linda Kirkland, Management Analyst

MONTANA LEGISLATIVE AUDIT DIVISION

PERFORMANCE AUDIT
Bankcard Transaction Fees and Contract Management
Department of Administration

JUNE 2015 14P-04 REPORT SUMMARY

State agencies processed payments totaling over $115 million using point-of-sale systems in fiscal year 2013 and $209 million online in calendar year 2013, which includes over $13 million in transaction fees paid by citizens and state agencies. The Department of Administration needs to improve its management of contracts to better assist agencies with resolving payment application issues, monitoring bankcard transaction fees, and monitoring contractor compliance with security requirements.

Context

Citizens are increasingly using credit and debit cards to purchase goods and services from state agencies. The Department of Administration (department) manages two term contracts to facilitate the processing of payments made through online and point-of-sale systems. One contract processes point-of-sale payments that are completed by customers at state agencies and universities. The other contract is required for payments that are processed online and is used by state agencies and the University of Montana. Montana State University uses a different contract to process online payments.

In fiscal year 2013 there were nearly 1.1 million transactions totaling over $115 million processed using point-of-sale systems. Transaction fees for this contract totaled nearly $2.2 million. There were approximately 6 million online transactions totaling $209 million processed during calendar year 2013. Audit work estimates online transactions fees totaled over $11.5 million.

Overall, audit work determined the department could improve its management of the two term contracts used to administer online and point-of-sale transactions statewide. Audit work found that while the department has improved its process for identifying and resolving problems when payment applications are being developed, improvements could be made to identifying and assisting agencies with problems that occur after implementation. We also found there is limited availability of statewide transaction fee data, which is important in understanding how these resources are used. Additionally, while security related to the processing of sensitive and confidential bankcard information is the responsibility of the contractor, the department should improve its monitoring of both contracts to ensure contractors are meeting security requirements.

Results

Audit work found the department needs to improve the management of its two term contracts. Recommendations relate to:

- Receiving and reviewing audits required as part of the point-of-sale contract that provide assurances the contractor is meeting security requirements.
- Developing a process to identify and resolve payment application issues.
- Developing a process for receiving and analyzing statewide transaction fee and convenience fee data.
- Developing a follow-up process on actions to be taken when contractor weaknesses or deficiencies are identified during the assessment of security controls.

(continued on back)

Recommendation Concurrence	
Concur	3
Partially Concur	0
Do Not Concur	0

Source: Agency audit response included in final report.

For a complete copy of the report (14P-04) or for further information, contact the Legislative Audit Division at 406-444-3122; e-mail to **lad@mt.gov**; or check the web site at **http://leg.mt.gov/audit**
Report Fraud, Waste, and Abuse to the Legislative Auditor's FRAUD HOTLINE
Call toll-free 1-800-222-4446, or e-mail **ladhotline@mt.gov**.

Chapter I – Introduction

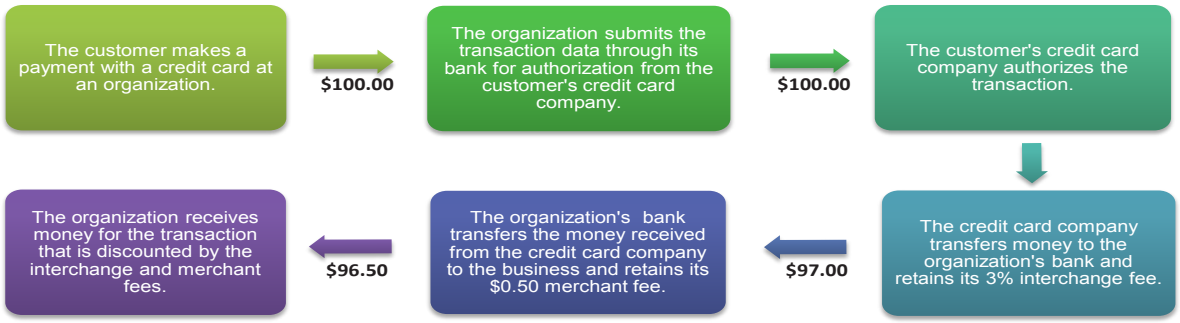
Introduction

Citizens are increasingly using bankcards to pay for government services such as renewing license plates, purchasing business licenses, and paying taxes. The acceptance of bankcards provides a variety of benefits to both state government and citizens. Benefits include improved customer convenience, decreased risk of cash theft, and improved operational efficiency. The Department of Administration (department) manages two term contracts for processing bankcard transactions at point-of-sale (POS) systems and online. The term contracts allow all state agencies to use the established contracts without going through an individual request for proposal process for each program they develop for POS or online payment processing.

The state processed transactions totaling over $115 million through POS systems in fiscal year 2013. Online transactions totaled over $209 million in calendar year 2013. However, these benefits are not without cost, which include transaction fees. Transaction fees for POS systems totaled nearly $2.2 million. The department and its contractor were unable to readily provide a breakdown of transaction fees for online payments. Audit work estimated transaction fees for online payments totaled over $11.5 million in 2013.

Transaction fees occur anytime bankcards are used to make a purchase at both private and public organizations. Interchange fees and merchant fees are two costs associated with accepting bankcards. Interchange fees are the fees charged by credit or debit card companies. These fees are a percentage of the purchase price and depend on the type of organization accepting the card, the method used to process the card, and the type of card used, among other factors. Merchant fees occur when the bank used by the organization to process bankcards charges a fee to acquire the money from the credit or debit card company. Merchant fees depend on the terms of the contract signed between the bank and the organization. The amount the organization ultimately receives is discounted by the amount of the interchange and merchant fees. Figure 1 (see page 2) illustrates the basic transaction fees that are associated with the processing of bankcards at any private or public organization.

Figure 1
Fees Associated with Processing Bankcards



Source: Compiled by the Legislative Audit Division.

Montana Electronic Government Services Act

The Montana Electronic Government Services Act addresses the establishment of electronic government services and fees. These statutes outline the responsibilities of the department and focus on the development of electronic government services. The department is required to:

- Provide the ability for state agencies to offer electronic government services by providing a reasonable and secure infrastructure.
- Provide a point of entry for electronic government services to achieve a single face of government.
- Encourage a common look and feel for all electronic government services for the benefit of the customers of the services.
- Set technological standards for electronic government services.
- Use technology that enables the greatest number of customers to obtain access to electronic government services.
- Promote the benefits of electronic government services through educational, marketing, and outreach initiatives.
- Share and coordinate information with political subdivisions whenever possible.

The department is allowed to contract with private entities in order to carry out the responsibilities outlined in the act. The department is also allowed to charge a convenience fee and may allow the contractor to collect the fee. This fee is in addition to the transaction fees which cover the merchant and interchange fees. The convenience fee on selected electronic government services is assessed to provide funding for the support and furtherance of electronic government services.

Security Over Processing Bankcard Transactions

Recent data breaches at major retailers and governmental agencies across the nation have highlighted the need to ensure security over bankcard information. There are two types of reviews completed related to the security of bankcard transactions processed in the state: Payment Card Industry Data Security Standards (PCI DSS) and service organization review. PCI DSS is a security audit that is required by credit card companies for any business that stores, processes, or transmits bankcard information. Service organization reviews are a recognized method that allow a service organization to provide a user entity with assurance over information that impacts the financial reporting at a user entity. This type of review provides assurance on financial controls over the processing of transactions and can also examine security controls at the service organization. The review can either examine the design of controls at the service organization or test the controls to ensure they are working as designed. Both reports provide the department and state agencies with information on security over the processing of bankcard information and the reliability of controls.

Audit Objectives

Based on our initial audit assessment of bankcard transactions conducted across state agencies, we developed two audit objectives:

1. Determine if the transaction fees charged to state agencies and citizens are accurate.
2. Determine if existing controls ensure the security of the public's bankcard information when using POS and online payment applications.

Audit Scope

Based on audit assessment work, we determined our work would focus on two areas. The first area examined was transaction fees. These are the costs associated with processing bankcards and consist of the fees charged by banks, credit card companies, and contracted private entities. These costs are paid by state agencies and/or citizens. We also included a review of the department's monitoring of security requirements because processing bankcards involves transmitting sensitive and confidential bankcard information electronically.

In our analysis of POS transaction fees, we examined two time frames. The first analysis reviewed the reasonableness of transaction fees during the second half of fiscal year 2013 (January through June 2013). This review included 35 POS systems operating at eight state agencies. The second analysis reviewed the percentage of change of transaction fees between fiscal years 2012 and 2013 to determine if there were

increases in transaction fees between the two years that required further examination. This analysis included state agencies and the university system.

In our analysis of online transaction fees, we reviewed transactions that occurred during the second half of fiscal year 2013. There were 81 active payment applications at the beginning of 2013 that allow for bankcard payments to be made online. We conducted a random sample of nine payment applications and received transaction data from the contractor to review. We contacted agency staff for the selected payment applications to discuss their reconciliation process for transactions. We also conducted two surveys of agencies that developed online payment applications within the last five years.

We examined the department's responsibilities for reviewing the contractors' security measures over processing bankcard transactions. Because transactions are processed by contractors, security is the responsibility of the contractor. However, the department is responsible for ensuring that independent audits are conducted on the contractors and reviewing whether contractors are meeting security requirements. We reviewed security audits completed on the online contractor during fiscal year 2013. Audit work also included a review of steps taken by the department to evaluate contractors' security.

Audit Methodologies

To address audit objectives, we conducted the following audit work:

- Reviewed statutes and administrative rules related to processing bankcards.
- Interviewed management and staff with the Procurement Bureau and State Information Technology Services Division of the Department of Administration.
- Reviewed the two contracts used to process bankcard transactions.
- Reviewed details of POS transactions processed for fiscal year 2013.
- Analyzed transaction fees on POS transactions during fiscal years 2012 and 2013.
- Interviewed state agency staff in programs processing POS transactions.
- Reviewed contractor reports on general development for 2011, 2012, and 2013, which included information on online transactions processed.
- Conducted a random sample of online payment applications active during the second half of fiscal year 2013.
- Analyzed transactions from the sampled programs and interviewed agency staff regarding their reconciliation process for transactions.

- Conducted a survey of payment applications developed in the last five years and asked agency staff questions about the development and reconciliation of these payment applications.
- Reviewed audit issues previously identified by financial compliance staff of the Legislative Audit Division.
- Reviewed two types of security reviews conducted by independent auditors.

Report Content

The following report includes three chapters addressing our audit findings, conclusions, and recommendations in the following areas:

- Chapter II examines transaction fees and security requirements related to POS payments.
- Chapter III examines transaction fees and security requirements related to online payments.

Chapter II – Point-of-Sale Transactions

Introduction

The point-of-sale (POS) contract was awarded in 2009 and renewed in 2014. This is a contract which is used, but not required, to process POS payments at state agencies. The State Information and Technology Services Division (SITSD) of the Department of Administration (department) currently manages this contract. Because a private entity is used to process these types of transactions for the state, the contractor charges a fixed fee of $0.08 per transaction. This fee is collected and retained by the contractor. Additionally, state agencies using the contract are responsible for paying the interchange fees. The interchange fees are the fees charged by the debit and credit card companies. They are variable based on the type of business accepting the card, the method used to process the card, and the type of card used, among other factors. An online reporting tool allows state agencies to view transaction revenues and fees for each merchant account.

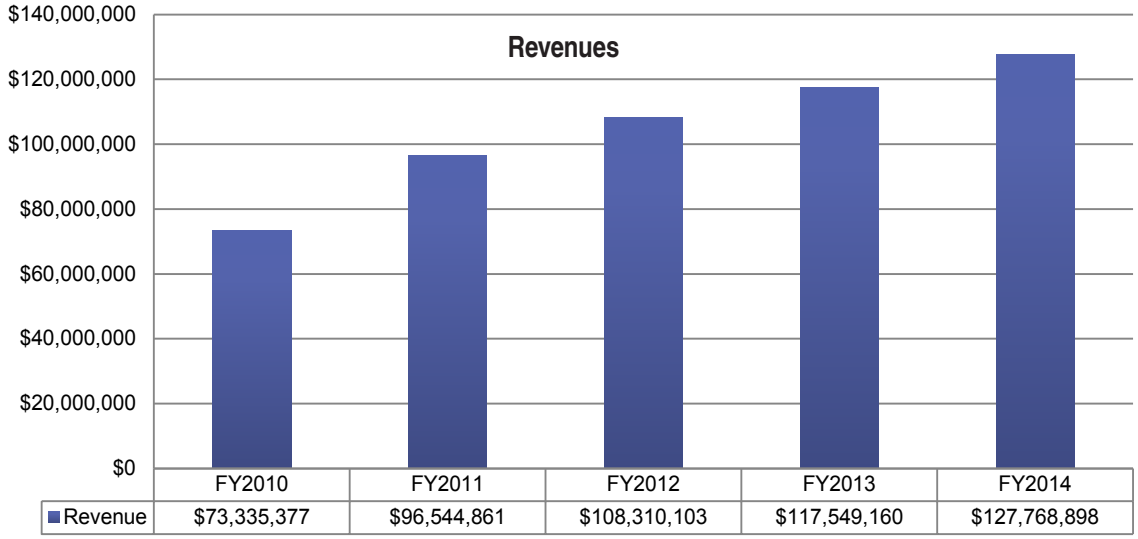
Per the POS contract, the contractor is required to demonstrate controls and safeguards over data and transactions maintained and processed on behalf of the state. The contractor is required to have an annual review of controls over the processing of payments completed each year while under contract, and is required to provide the department copies of all reports throughout the contract period on April 30, unless an alternate date is agreed upon. The contract also requires necessary controls be maintained to ensure compliance with security requirements. The contract requires a comprehensive security program that is audited each year to validate compliance with industry security standards for protecting bankcard transactions.

Our first objective was to determine if transaction fees charged to state agencies and citizens are accurate. Based on audit work, we determined controls are in place to ensure accuracy of POS transactions. Our second objective was to determine if existing controls ensure the security of the public's bankcard information when using POS systems. We identified areas where the department could enhance its monitoring of controls to ensure efforts in this area are effective.

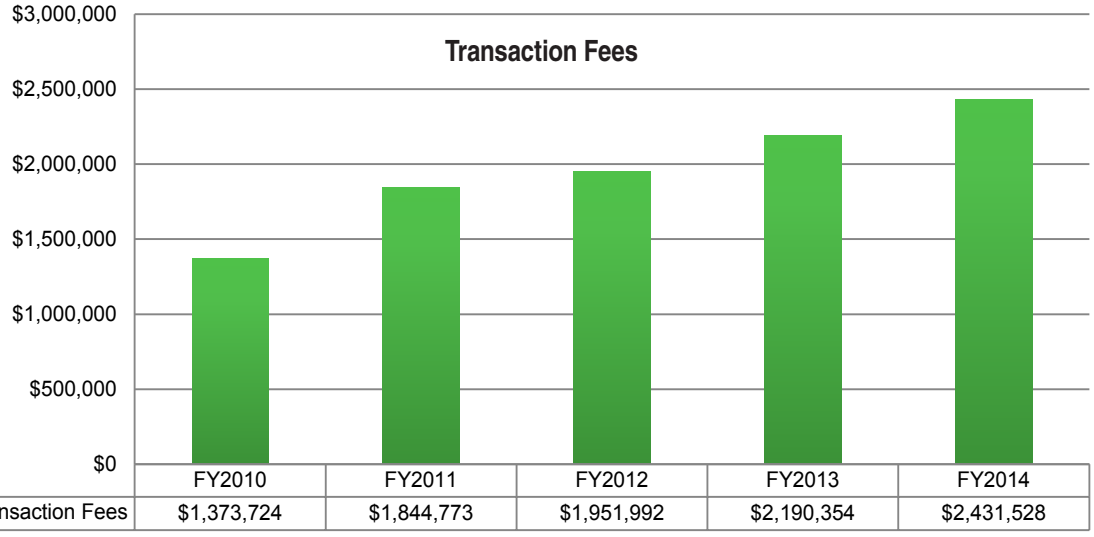
Point-of-Sale Transactions

In fiscal year 2013, there were 35 POS systems at state agencies and 192 POS systems at Montana State University and University of Montana. In fiscal year 2013, state agency and university POS systems processed nearly 1.1 million transactions totaling over $115 million. Transaction fees totaled nearly $2.2 million. Figure 2 (see page 8) illustrates the growth of transaction revenues and fees processed at state agencies and the university system over the course of five years.

Figure 2
Point-of-Sale Transaction Revenues and Fees
Fiscal Year 2010 through 2014



	FY2010	FY2011	FY2012	FY2013	FY2014
Revenue	$73,335,377	$96,544,861	$108,310,103	$117,549,160	$127,768,898



	FY2010	FY2011	FY2012	FY2013	FY2014
Transaction Fees	$1,373,724	$1,844,773	$1,951,992	$2,190,354	$2,431,528

Source: Compiled by the Legislative Audit Division from information provided by the department.

As part of our audit work we interviewed staff at five state agencies regarding the processing of POS transactions. Table 1 (see page 9) shows state agencies processed over 120,000 transactions totaling nearly $13 million in fiscal year 2013. These transactions are made through POS terminals at agencies. Agency staff use receipts generated by the POS machine at the time of the transaction or spreadsheets developed by staff to record transactions at the time of purchase to reconcile. These agency records are

compared to monthly statements provided by the contractor to ensure the accuracy and completeness of deposits made to the state treasury.

Table 1
Point-of-Sale Transactions at State Agencies
Fiscal Year 2013

State Agency	Number of Point-of-Sale Systems	Number of Transactions	Revenue
Department of Fish, Wildlife and Parks	22	34,643	$2,322,135
Department of Transportation	3	77,871	9,747,864
Montana Historical Society	3	4,031	257,163
Department of Administration	2	676	441,412
Department of Commerce	2	2,728	76,271
Department of Corrections	1	658	92,145
Office of Public Instruction	1	22	6,613
Secretary of State	1	244	13,607
Total	**35**	**120,873**	**$12,957,210**

Source: Compiled by the Legislative Audit Division from information provided by the department.

Analysis of Interchange Fees

Interchange fees are amounts charged by credit card companies and are a percentage of the transaction amount. The percentage is variable and based on many factors, including the type of business accepting the card, type of card used, and method used to process the card. As part of the contract, interchange fees are passed from the credit card companies to agencies.

The Government Finance Officers Association, an organization that reviews public policy related to the management of governmental financial resources, reported that fees range from 1 to 3 percent. As part of our audit work, we set our threshold for review at 3 percent. We reviewed interchange fees at state agencies from January 2013 through June 2013. During this period, there were over 57,000 transactions processed totaling $6.5 million. Interchange fees totaled over $129,000.

As seen in Table 2 (see page 10), the majority of the interchange fees were between 1.25 percent and 2.75 percent. There were only 14 out of 57,000 transactions that were greater than three percent. These transaction fees totaled $46 so no further work was

conducted because the number of transactions and amount of interchange fees were minimal.

Table 2
Interchange Fees Charged at State Agencies
January 2013 through June 2013

Interchange Fee Percentages	Total Interchange Fees	Percentage of Total Interchange Fees	Number of Transactions	Percentage of Total Number of Transactions
Less than 0.50%	$ 1,717	1%	6,647	12%
0.50% - 1.00%	4,954	4%	6,897	12%
1.00% - 1.25%	278	0.21%	705	1%
1.25% - 1.50%	13,259	10%	7,913	14%
1.50% - 1.75%	10,160	8%	6,945	12%
1.75% - 2.00%	1,433	1%	1,079	2%
2.00% - 2.25%	10,798	8%	4,634	8%
2.25% - 2.50%	42,879	33%	12,110	21%
2.50% - 2.75%	38,379	30%	9,334	16%
2.75% - 3.00%	5,667	4%	760	1%
Greater than 3.00%	46	0.04%	14	0.02%
Total	**$129,570**	**100%**	**57,038**	**100%**

Source: Compiled by the Legislative Audit Division from information provided by the department.

Analysis of Transaction Fees

We reviewed the percentage of change in transaction fees between fiscal years 2012 and 2013. Our review examined the percentage of change for transaction fees, revenues, and the number of transactions by month between each year. For example, we compared the percentage of change between February 2012 and February 2013. We used this method in order to review cyclical transactions more closely. Information provided by the contractor was used to calculate the percentage of change by month between fiscal years 2012 and 2013 for transaction fees, revenues, and the number of transactions. We identified and examined outliers in each of these areas.

Once the outliers were identified, it was important to look at the relationships between all of these factors. For example, an outlier in revenues may indicate that one merchant's sales increased at a much higher rate than the sales for other merchants. This may correspond to a percentage increase in the number of transactions and transaction

fees for that merchant which would also cause those fields to be outliers. If all of these fields increased and transaction fees were within an acceptable range, there would be no cause for concern. In our analysis of outliers we looked at the relationship between percentage of change between:

- Transaction fees and revenues.
- Transaction fees and the number of transactions.
- Revenues and the number of transactions.

In our analysis, there were 42 instances where the difference between transaction fees and revenues warranted a closer review; 46 instances where the difference between transaction fees and the number of transactions required review; and 16 instances where the difference between revenues and the number of transactions warranted further examination. We determined none of these outliers were an audit issue. The majority of the reasons for the difference in the percentage of change included:

- A new monthly fee charged by a credit card company which began in April 2012.
- No transactions in fiscal year 2012, which skewed the percentage of change between fiscal years 2012 and 2013.
- A significant increase (and in one case a significant decrease) in revenue generated by bankcard transactions.

There is a large variety in the amount of transaction fees charged by the banks and credit cards companies for any organization processing bankcards. These fees depend on the type of organization accepting the card, the method used to process the card, and the type of card used, among other factors. Agencies are provided with monthly statements detailing revenues and fees for transactions processed. The information allows agencies to ensure the accuracy of revenues and the reasonableness of transaction fees. In our analysis, we did not identify concerns regarding the interchange fees charged during the second half of fiscal year 2013 and the percentage of change in transaction fees between fiscal years 2012 and 2013. We have reasonable assurance that when citizens are using credit and debit cards at state agencies to make purchases, state agencies are receiving accurate revenues and paying correct transaction fees.

Conclusion

The availability of agency transaction records and readily-accessible information on transaction activity from the contractor allow for independent reconciliation of revenue amounts and a reliable reporting of transaction fees under the point-of-sale contract.

Security of Point-of-Sale Payments

The POS contract processes nearly 1.1 million transactions in fiscal year 2013 at agency and university POS systems. According to department staff, the contractor operates its own secure network to process payments and does not have servers connected to the state's network. The POS terminals operate through connection to the internet. As such, the state relies on the contractor to manage its own security. The service organization review and security audit reports are methods available for the department to verify the contractor's compliance with security requirements.

Review of Contractor Controls

As part of our audit work, we intended to review the contractor's service organization review, which is conducted by an independent auditor. This type of review expresses an opinion on the fairness of the description, suitability of design, and operating effectiveness of controls. The contractor is required to demonstrate controls and safeguards over bankcard data and transactions maintained and processed on behalf of the state. The review is required to be completed annually while the contract is in place. The contractor is required to provide the department with copies of all reports throughout the contract period by April 30, unless an alternate date is agreed upon.

When the contract was initially awarded, the department received the 2009 service organization review. However, the department had not received copies of the reviews from 2010 through 2014. When the department requested the contractor provide the reviews, the contractor required the department to sign a nondisclosure agreement before the reviews could be sent due to their confidential nature. After the conclusion of audit work, the department was able to come to a consensus on the language in the nondisclosure agreement and received the reviews.

Audit of Security Requirements

As part of our audit work, we also intended to review documentation of compliance with security requirements. The contract requires the contractor maintain a comprehensive security program that is audited each year to validate compliance with Payment Card Industry Data Security Standards (PCI DSS). While the contract does not require the contractor provide the state with copies of these audit reports annually, it is required to provide documentation of compliance when requested. When the department requested documentation of compliance with security requirements, like the report reviewing controls, the contractor required the department to sign a nondisclosure agreement before the reports could be sent. The department was not able to obtain documentation of compliance during our audit; however, after the conclusion of audit work, the department and the contractor reached a consensus on the nondisclosure agreement and the department will obtain documentation.

Contract Management Responsibilities

The provision of the contract requiring the contractor to provide a report on the review of controls to the department has not been enforced by the contract manager. The only report received was in 2009 and reports have not been received from 2010 through 2014. The new contract manager, who had been managing this contract since March of 2014, was not familiar with this contract and had not requested the 2014 audit report. Additionally, the contract requires the necessary controls are met to ensure PCI DSS compliance. While the contract does not require this audit be provided annually to the state, it should be available upon request. Without documentation of the contractor's security controls, state agencies have limited assurance on the security of the system used to process transactions. Service organization reviews provide information on contractors' controls related to certain aspects of security. Additionally, PCI DSS compliance ensure the contractor meets established security requirements for all companies that process, store, or transmit credit card information. Without verification of compliance with contract provisions, the state risks potentially exposing banking information for the nearly 1.1 million transactions processed through this contract. If bankcard information was exposed, this would hurt the confidence citizens have using bankcards to make purchases at the state.

RECOMMENDATION #1

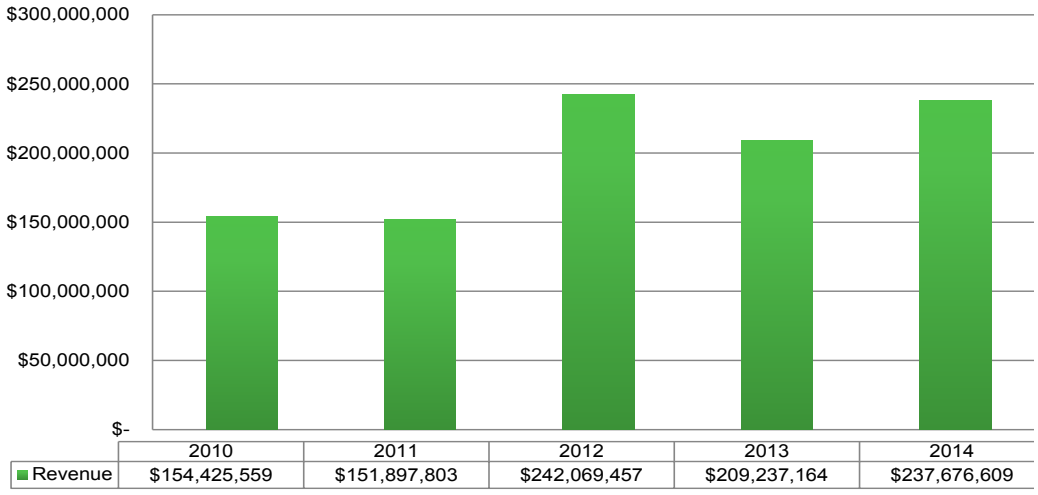
We recommend the Department of Administration enforce contract provisions by receiving and reviewing the service organization review and documentation of Payment Card Industry Data Security Standards compliance annually to verify the contractor's compliance with security requirements.

Chapter III – Online Transactions

Introduction

The online contract, initially awarded in 2001 and awarded again in 2011, is managed by the State Information and Technology Services Division (SITSD) of the Department of Administration (department). The contractor develops payment applications for programs within state agencies to allow customers to purchase goods and services online from agencies. The number of transactions processed through the online contract continues to increase and will likely continue as more services are developed and more people move to purchasing government services online. The figure below illustrates growth from 2010 through 2014. Transaction fee data on a statewide basis is not included in this figure because neither the department nor the contractor had this information readily available.

Figure 3
Online Transaction Revenues
Calendar Year 2010 through 2014



	2010	2011	2012	2013	2014
Revenue	$154,425,559	$151,897,803	$242,069,457	$209,237,164	$237,676,609

Source: Compiled by the Legislative Audit Division from information provided by the department.

Our first objective was to determine if transaction fees charged to state agencies and citizens are accurate. We identified areas where management of the contract could be improved to better monitor transaction fees. Additionally, our second objective was to determine if existing controls ensure security of the public's bankcard information when using online payment applications. Audit work found the department needs to improve its follow-up process for vulnerabilities identified during its scan of online payment applications and servers.

Transaction Fees

Transaction fees are outlined in work orders with individual agencies. These work orders typically have a flat fee to cover merchant fees, a percentage of the transaction amount to cover interchange fees, and convenience fees paid to the contractor. The merchant fee is $0.25 per transaction. Interchange fees for most bankcards processed are 1.995 percent of the transaction amount. There is one type of card that has a higher rate at 2.15 percent of the transaction amount. Additionally, the development and maintenance of the online applications are completed by adding an additional transaction fee, called a convenience fee. The convenience fee is typically $1.00 but can vary depending on the payment application.

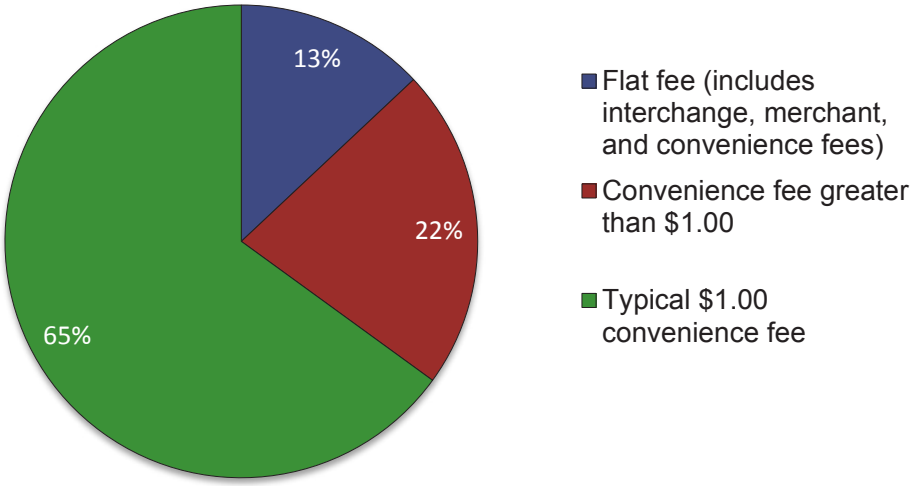
Transaction Fees Established in Work Orders

State agencies using the online term contract create individual payment applications using work orders to provide specifications for payment applications. The work orders outline the work to be completed, development schedule, and fees collected, among other requirements. The department has been working with agencies and the contractor to improve communication regarding expectations. A few of these improvements include additional documentation in work orders of the timeline to complete projects, documentation of change and enhancement requests for applications, and biweekly status reports which track the progress of applications that are in the process of being developed.

Each payment application has individual requirements outlined in the work order. Agencies individually determine how they want to handle fees, so interchange, merchant, and convenience fees can vary between agencies. As part of our audit work, we conducted a survey of state agency staff on the development of online payment applications. The survey included online payment applications developed between 2009 and 2013. The survey results in Figure 4 (see page 17) show that 35 percent of payment applications have transaction fees and/or convenience fees that are different than the typical fee schedule. One of these applications has a flat fee of 2.5 percent which covers the interchange and merchant fees, and the convenience fee paid to the contractor is the typical $1.00 fee. Two applications pay a flat fee that covers the interchange, merchant, and convenience fees. The remaining five agencies pay convenience fees to the contractor which are greater than the $1.00 convenience fee agencies are typically charged.

Figure 4

Convenience Fee Schedule for Surveyed Payment Applications



Source: Compiled by Legislative Audit Division.

Survey results also indicate there is confusion among state agency staff related to how convenience fees are established and who is responsible for determining these fees. According to department staff, their expectation is that the convenience fee is established through a discussion between the agency, department, and the contractor. Higher convenience fees are based on the amount of work required to meet the agency's needs and the transaction volume expected, and are determined on a case-by-case basis. However, decisions on how the amount of the convenience fee is established are not documented.

Analysis of Online Payment Application Survey Results

As part of our audit work, we developed a survey to examine the reconciliation of online transactions. The survey included online payment applications developed between 2009 and 2013. Respondents were asked to provide a description of how their agencies track transaction information independent from the information provided by the contractor, as well as an overview of the entire reconciliation process. When the responses to these two questions were evaluated in conjunction with one another, only 33 percent (6 out of 18) of the respondents provided an overview of the reconciliation process that included independent information. The majority of the responses included comparing information of the amount deposited by the contractor to transaction information provided by the contractor. There was no verification with agency data to ensure the amount the contractor is depositing is the amount that should be deposited.

Analysis of Sampled Online Payment Applications

Additionally, we conducted a random sample of 9 out of 81 online payment applications developed for state agencies (excluding the University of Montana). We reviewed transactions from January 2013 through June 2013. We found five of the nine payment applications reviewed do not have enough information to allow agencies to track transaction information independently from the information provided by the contractor. One of the agencies in our sample found discrepancies during its reconciliation process. For fiscal years 2014 and 2015, there were reconciliation discrepancies that had not been resolved. For fiscal year 2014, the agency determined there was over $12,000 owed to it according to information included in its database. For the first three months in fiscal year 2015, there was nearly $6,000 owed to the agency according to its records. There was no resolution to these outstanding amounts.

In the case of our sample, there were limited controls in place to ensure that over $3.2 million in transaction revenue was correctly received by the contractor or collected by the agencies from January 2013 through June 2013. The department needs to improve its ability to identify issues agencies are facing and assist them in resolving these problems. The department identified the inability of some agencies to reconcile transaction data with independent data as a weakness from the onset of the contract in 2001. Currently, there is limited information on the number of payment applications without the ability to independently reconcile transaction data and limited communication of reviews that may provide agencies with assurances over revenue and fees. For example, the contractor has an annual independent audit of its financial statements that reviews a sample of the transaction data. The department needs to determine if the sample provides assurances over transaction data provided by the contractor and how to communicate these assurances to agencies.

Availability of Transaction Fee Data

The Montana Electronic Government Services Act allows the department to contract with private entities to develop electronic government services which includes online payment applications. In order to support these services and the development of additional services, the department may charge a convenience fee. The online payment processing contract requires the majority of projects to be funded through this type of fee structure, which is called transaction-based self-funding. This means that convenience fees are used statewide for the development and maintenance of online payment applications. This fee is typically $1.00 per transaction processed but is determined on a case-by-case basis depending on the type of service provided.

The availability of statewide information regarding bankcard transaction fees is limited. While the department retains copies of individual work orders, this information is

not compiled in a way that allows the department to review the fee structure across state agencies. The department requires the contractor to submit quarterly reports that include basic financial statements and high-level transaction data. However, the transaction fee data is not broken out between general transaction fees, which would include the interchange and merchant fees, and convenience fees. The contractor and department were not able to readily provide this fee information.

Contract Management Responsibilities

The online contract designates contract and project management roles for department staff. Responsibilities for the contract manager include being the single point of contact where written notices, requests, complaints, or any other issues regarding the contract should be directed. Project management responsibilities include day-to-day project management on behalf of the state. The online contract is between the department and the contractor, and because this is a term contract, it is established for all state agencies to use when processing bankcards.

The Montana Operations Manual policy addresses post-award obligations on how state agencies should manage contracts. Specifically, this policy requires each state agency to have a system in place to monitor its own contracts. In addition, this policy establishes expectations regarding contract enforcement by maintaining that agencies need to "place a tremendous emphasis on effective contract administration. On a day-to-day basis, agencies need to be monitoring contract performance since early detection and correction of nonperformance is critical for the success of the contract."

The Montana Operations Manual has a policy regarding internal controls which, among other things, outlines management responsibilities. One part of internal controls provides accountability in managing resources. The manual maintains that public officials, legislators, and taxpayers are entitled to know whether government funds are handled properly and in compliance with applicable laws and regulations. They need to know whether government organizations, programs, and services are achieving the objectives for which they were authorized and funded.

Controls Over Online Transactions Could Be Improved

While the department has improved its process for establishing and resolving problems identified when payment applications are being developed, improvements could be made to identify issues agencies have after implementation. As the contract manager, the department has a responsibility to identify and assist agencies in resolving issues. Assisting agencies with resolving problems, such as the inability to reconcile transaction data, improves contract monitoring. The more problems that are resolved, the more assurances agencies and the department have that the contract is working as intended.

Currently, there are limited processes in place to monitor and analyze transaction fees on a statewide basis. Financial statements provide aggregate transaction fee information. Neither the department nor the contractor were able to readily provide information on the amount of convenience fees on a statewide basis. Audit staff estimate convenience fees to be approximately $6 million in fiscal year 2013. Because these fees vary between agencies, it is important to track and monitor how these fees change and grow over time. This would assist the department in understanding how these resources are used and would assist in identifying any concerns about how these fees are applied across state agencies. Additionally, analyzing transaction and convenience fees on a statewide basis would provide the department with information that would assist in assessing contract renewal in 2018. Currently, the department does not receive or monitor this information and potentially could lose public trust that these fees are handled properly.

RECOMMENDATION #2

We recommend the Department of Administration improve its management of the contract for online transactions by:

A. *Developing a process to identify payment application issues on an ongoing basis and assist agencies with resolving problems.*

B. *Developing a process for receiving and analyzing statewide transaction fee and convenience fee data.*

Security of Online Payments

The online contract is an exclusive contract with the state for processing online payments. In calendar year 2013, the contractor processed an estimated 6 million transactions totaling $209 million for state agencies and the University of Montana. According to agency staff, the contractor has two servers that reside at the Information Technology Services Divisions data center. These servers operate on the state network in the demilitarized zone (DMZ). The DMZ is a separate area on the network for servers. It provides access to users outside the network to information systems that reside on the network.

Audit of Controls and Security Requirements

As part of our audit work, we reviewed the annual service organization review completed on the parent company of the contractor. This report expressed an opinion on the fairness of the description, the suitability of design, and operating effectiveness of controls over the parent company's Transaction Payment Engine. When a transaction

is initiated online by a customer, the Transaction Payment Engine is used to receive authorization to process the payment. The audit reviewed several controls related to the payment engine and its security. The opinion issued by the auditors stated in all material respects the controls were fairly presented and operating effectively. However, the report indicated that certain control objectives can only be achieved if user entity controls are suitably designed and operating effectively in conjunction with the service organization's controls.

As part of our audit work, we also reviewed documentation related to the contractor's compliance with security requirements. The contractor completed a self-assessment questionnaire. This questionnaire can be a part of the Payment Card Industry Data Security Standards (PCI DSS) assessment process and the organization self-evaluates compliance with six control objective requirements by addressing specific questions related to them. This self-assessment questionnaire did not identify any vulnerabilities related to PCI DSS. In addition to completing the questionnaire, the contractor had a scan conducted by a third-party vendor to attest to compliance with security requirements. This report states the contractor passed the review.

Vulnerability Scans

The contractor's servers reside on the DMZ area of the state network. Because these servers reside on the state network, SITSD conducts vulnerability scans annually on the servers and the applications included on the servers. Vulnerabilities are areas within a system that can potentially be exploited and/or threatened and lead to data breaches. We reviewed the vulnerability scans completed on the servers and applications. The vulnerability scans reviewed were conducted in November 2014 and found the following vulnerabilities:

Network Scan

- 2 medium vulnerabilities
- 4 low vulnerabilities
- 46 informational vulnerabilities

Web Scan

- 16 informational vulnerabilities

The severity of vulnerabilities for this type of scan have a range of critical, high, medium, low, and informational. All vulnerabilities detected need to be reviewed in relation to one another. Several low risk vulnerabilities may elevate to a level of concern when they are combined if they are effecting a similar area.

Contract Management Responsibilities

Department policy addresses both network security as well as security assessment and authorization. The first policy addresses network security for information systems that SITSD manages or controls, including systems that third-parties manage or host on SITSD's behalf. This policy identifies several requirements related to the DMZ. These responsibilities include maintaining documentation on all devices in the DMZ that show proof of a security or vulnerability check before access is allowed and the devices are moved into production mode.

Additionally, there is a department policy that establishes the requirement of SITSD to implement security assessment and authorization for systems SITSD manages and controls, including systems that third-parties manage or host on SITSD's behalf. Specific requirements of SITSD include:

- The assessment of security control effectiveness and documented report of the results of the assessment.
- The authorization of information systems by a senior level executive to ensure risks have been mediated or accepted before commencing operations.
- The ongoing monitoring of security controls and the security state of the information systems.
- Develop and update, on an ongoing basis, a plan or action and milestones for the actions that will be taken to correct weaknesses or deficiencies noted during the assessment of security controls.

The contract is for a system that is managed by the contractor on SITSD's behalf. This requires continued assessment and monitoring of security controls. Additionally, if issues are found, a plan of action and milestones are required to correct weaknesses or deficiencies noted during the assessment of the security controls. Therefore, SITSD should be obtaining documentation from the contractor on the plan to correct vulnerabilities detected during SITSD's scans.

While the department takes an active role reviewing the control and security audit reports, staff does not follow up when vulnerabilities are detected during scans of the contractor's servers and applications. According to SITSD staff, since the servers belong to the contractor, it is the contractor's responsibility to complete a corrective action plan. Staff stated that SITSD has its own corrective action plan process, but it only pertains to its own applications, services, and equipment. Staff were not sure of the contractor's process. The belief is that the contractor is taking an active stand on monitoring its own system. However, the contractor is processing 6 million transactions totaling $209 million on behalf of the state. Without a process for ensuring vulnerabilities are corrected, there is potential that a vulnerability may lead to a breach of citizens'

bankcard information. Additionally, since the contractor's servers are connected to the network, there is the potential these vulnerabilities could lead to a data breach on the state's network.

RECOMMENDATION #3

We recommend the Department of Administration develop a follow-up process on actions to be taken when contractor weaknesses or deficiencies are identified during the assessment of security controls.

Department of Administration

Department Response

MONTANA DEPARTMENT OF ADMINISTRATION
"the backbone of state government"

Director's Office
Steve Bullock, Governor • Sheila Hogan, Director

June 4, 2015

Ms. Tori Hunthausen
Legislative Auditor
State Capitol Building, Room 160
Helena, MT 59620

RE: Audit 14P-04 Bankcard Transaction Fees and Contract Management

Dear Ms. Hunthausen:

Thank you for the opportunity to respond to the Bankcard Transaction Fees and Contract Management performance audit. We appreciate the work of both Katherine Guenther and Joe Murray, who were very professional and thorough in their review.

Following is the Department of Administration's response:

Recommendation #1
We recommend the Department of Administration enforce contract provisions by receiving and reviewing the service organization review and documentation of Payment Card Industry Data Security Standards compliance annually to verify the contractor's compliance with security requirements.

Department Response:
Concur. The department's contract manager has received and reviewed the contractor's 2014 audit report. The contract manager will continue to request and review audit reports annually.

Recommendation #2
We recommend the Department of Administration improve its management of the contract for online transactions by:

A. Developing a process to identify payment application issues on an ongoing basis and assist agencies with resolving problems.

B. Developing a process for receiving and analyzing statewide transaction fee and convenience fee data.

Department Response:

A. Concur. The contract manager is now the point of contact for agency issues and has enforced provisions of the contract that require no later than next business day response from the contractor on agency issues. The contract manager is responsible for tracking issues through resolution.

B. Concur. The State Information Technology Service Division's internal auditor, working with the State Financial Services Division, is in the process of reviewing statewide transaction fee and convenience fee data and will make a recommendation to the Chief Information Officer by late fall.

Recommendation #3:

We recommend the Department of Administration develop a follow-up process on actions to be taken when contractor weaknesses or deficiencies are identified during the assessment of security controls.

Department Response:

Concur. The department has developed and put in place a follow-up process on actions to be taken if contractor weaknesses or deficiencies are identified during the assessment of security controls.

Again, Director Hogan and I appreciate the auditors' work and look forward to implementing the recommendations.

Sincerely,

Mike Manion

Michael P. Manion, Deputy Director